CLAIMS

1-15 (canceled)

16 (previously presented) A method for monitoring a security parameter for a network by tracking changes to the contents of system files, the network having a first and a second server, the first server having a transport mechanism communicatively connected to the second server, the method comprising the steps of:

monitoring at one or more times for changes to a firewall policy;

collecting on the first server the changes to the firewall policy;

storing the changes to the firewall policy on the first server;

compiling a history of the changes to the firewall policy on the first server;

reporting the history of the firewall policy changes; and

the second server performing other networking tasks concurrently with the steps of collecting, storing, compiling, or reporting.

17 (previously presented) The method of step 16, further comprising the steps of:

monitoring whether a change is an approved change; and

archiving changes into a first report, the report identifying approved changes.

18 (original) The method of claim 17 further comprising the steps of:

monitoring information on an administrator of a networking policy change;

collecting information on the administrator of the networking policy changes;

archiving one or more sets of information on the administrator; and

compiling the one or more sets of information on the administrator of the networking policy changes, the user able to view the compiled information in a format determinable by the user.

19 (original) The method of claim 18 further comprising the steps of:

monitoring the time of the administrator's networking policy changes;

collecting the time of the administrator's networking policy changes;

archiving one or more sets of times of the administrator's networking policy changes; and

compiling the one or more sets of time of the administrator's networking policy changes, the user able to view the compiled time in a format determinable by the user.

20 (original) The method of claim 19 further comprising the steps of:

collecting the firewall policy change that is pushed to the firewall policy;

archiving one or more sets of firewall policy information that is pushed to the firewall policy; and

compiling the one or more sets of firewall policy information that is pushed to the firewall policy, the user able to view the compiled firewall policy information that is pushed in a format determinable by the user.

21 (previously presented) The method of claim 20 further comprising the steps of:

establishing one or more baselines by an administrator for a system on the network;

monitoring the one or more baselines established by an administrator;

collecting information on changes to the one or more baselines into a baseline report;

archiving one or more baseline reports of the changes; and

compiling the one or more baseline reports, the user able to view the compiled information in a format determinable by the user.

22 (previously presented) The method of claim 21 further comprising the steps of:

monitoring one or more operating system's file integrity on the network;

collecting information on changes to the one or more operating system's file integrity into a file integrity report;

archiving the one or more file integrity reports; and

compiling the one or more file integrity reports, the user able to view the compiled information in a format determinable by the user.

23 (previously presented) The method of claim 22 further comprising the steps of:

monitoring a Web server's configuration file;

collecting information on changes to the Web server's configuration file into a Web Server's configuration report;

archiving the one or more Web Server's configuration reports; and

compiling the one or more Web Server's configuration reports, the user able to view the compiled information in a format determinable by the user.

24 (previously presented) The method of claim 23 further comprising the steps of:

monitoring a proxy server's configuration file;

collecting information on changes to the proxy server's configuration file into a proxy server's configuration file report;

archiving the one or more proxy server's configuration file reports; and

compiling the one or more proxy server's configuration file reports, the user able to view the compiled information in a format determinable by the user.

25 (previously presented) The method of claim 24 further comprising the steps of:

monitoring a user's password strength;

collecting information on the password's strength into a password strength report;

archiving the one or more password strength report; and

compiling the one or more password strength report, the user able to view the compiled information in a format determinable by the user.

26 (previously presented) The method of claim 25 further comprising the steps of:

establishing one or more events that triggers an alert;

monitoring for the one or more alert triggering events;

providing an alert notice upon the occurrence of the one or more alert triggering event;

27 (original) The method of claim 26 further comprising the steps of:

collecting information on the one or more alert triggering event into a alert report;

archiving the one or more alerts reports; and

compiling the one or more alert reports, the user able to view the compiled information in a format determinable by the user.

28 (original) The method of step 27 further comprising the step of:

monitoring encrypted secure connections between the first and the one or more second servers.

29 (withdrawn) A method for providing notice of system vulnerabilities to a system administrator, the method comprising the steps of:

providing system users with one or more downloadable preconstructed baseline templates;

providing md5sum information for applications thereby allowing users use of preconstructed templates;

providing means for notification to the user of software or hardware that contains a vulnerability;

inserting an alert notice in the templates regarding the vulnerability;

noting the alert notice in the template when a baseline engine is run;

verifying a file version; and

alerting an administrator of the vulnerability.

30 (withdrawn) A method for generating and gathering system configuration data for audits comprising the steps of:

generating data on system configuration changes;

generating statistical samplings of changes for comparison against certain predetermined criteria; and

providing information on comparison data, average number of changes, or total changes made to a system administrator.

31 (withdrawn) The method of claim 30 wherein the statistical samplings of changes are generated when the number of changes occurring are too numerous to verify manually.

32 (withdrawn) The method of claim 30 further comprising the step of generating a report on the total number of system changes for a given time period.

33 (withdrawn) A method of using a search module in a system to search for particular information comprising the steps of:

storing all pre-determined system configuration information in a searchable central database; and

finding actual system configuration information in any of a plurality of sub-systems monitored by the system, thereby allowing for quick resolution of configuration problems in large network environments by providing auditors with the ability to examine only information that is pertinent to the specific problem.

34 (withdrawn) A method for checking the validity of critical files comprising the steps of:

triggering system execution;

checking the md5sum of one or more critical files;

verifying the md5sum of the one or more critical files against a known value;

continuing system execution only if the md5sum matches the known value.

35 (previously presented) A method for providing a security policy watch comprising the steps of:

pre-configuring standard system alerts that adhere to preexisting corporate security policies;

determining whether a firewall policy complies with pre-existing corporate security policies; and

generating an alert when a firewall policy is determined not to comply.

36 (previously presented) The method of claim 35 further comprising the step of determining whether a system is within certain predetermined corporate guidelines with respect to particular types of software packages, particular versions of specific software, particular hardware, or processor speed.

37 (previously presented) A method for monitoring changes made to systems comprising the steps of:

recording information on scheduled system changes on a central server log;

storing scheduled change information in a central database;

detecting actual system changes when they are made to the system;

transporting actual system change information to a central database;

providing for comparison of scheduled change information and actual change information thereby allowing auditors to detect system change errors and system tampering.